KUTAKROCK

kutakrock.com

HIPAA Privacy Rule Overview and Hot Topics

Marceda M. Starks

Kutak Rock LLP


NANCY, I'M NOT SURE THAT'S WHAT HIPAA HAD IN MIND.

Outline

- Overview of HIPAA Privacy Rule
- Business Associate Agreement
- Breach and Breach Notification Rule

"No, it's not a female Hippopotamus, anyone else know?"

HIPAA Key Terminology

HIPAA

- HIPAA – Health Insurance Portability and Accountability Act
- HITECH – Health Information Technology for Economic and Clinical Health Act, passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA)
- PHI – Protected Health Information
- CE – Covered Entity – health care provider, health plan, health care clearing house
- BA – Business Associate – person or entity who performs work on behalf of CE and is not a member of its workforce. Such work or services must involve the use or disclosure of PHI
- BAA – Business Associate Agreement – An agreement between the CE and BA about HIPAA
- TPO – Treatment, Payment, Health care operations

Core Elements of HIPAA

- The Privacy Rule – Establishes individuals' privacy rights and addresses the use and disclosure of PHI by covered entities and business associates.
- The Security Rule – Establishes requirements for protecting electronic PHI.
- The Breach Notification Rule – requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI.
- The Enforcement Rule – Establishes both civil monetary penalties and federal criminal penalties for the knowing use or disclosure of PHI in violation of HIPAA.

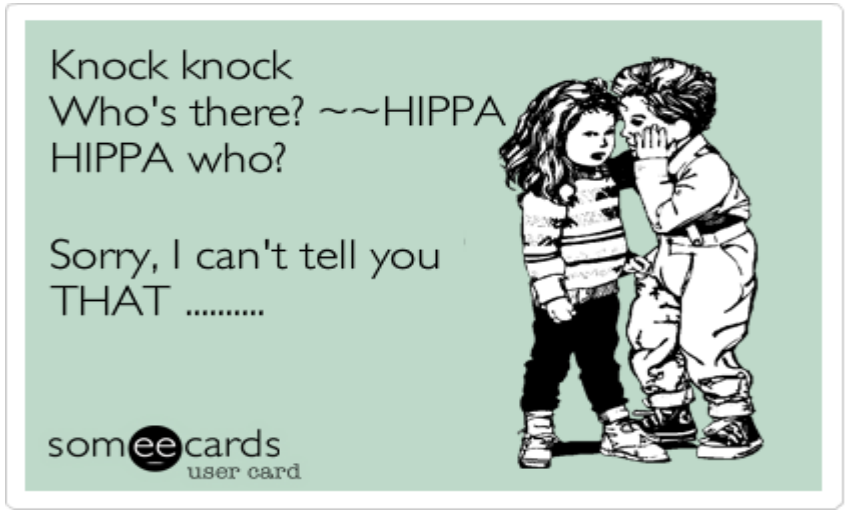
KUTAKROCK

When Does HIPAA Apply

- HIPAA applies when there is a Covered Entity or Business Associate involved with the access, use, disclosure, receipt or maintenance of PHI.

What is the HIPAA Privacy Rule

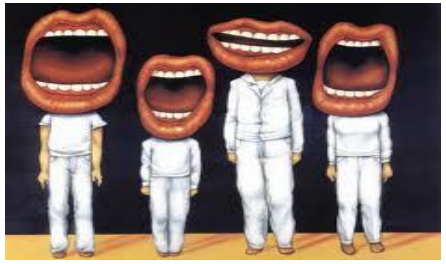
- The Privacy Rule
  - A Covered Entity or Business Associate may not use or disclose Protected Health Information (PHI) unless:
    - Authorized by the individual who is the subject of the information;
    - Permitted by the regulations; or
      - You may use and disclose PHI for treatment, payment, and health care operations without an authorization.
    - Required by the regulations.



KUTAKROCK

What is PHI?

- PHI is any information that:
  - Is **created**, **maintained, transmitted**, or **received** by a CE
  - Relates to an individual's **past**, **present**, or **future physical** or **mental health** or **condition**, **receipt of health care**, or **payment for health care**; and
  - Identifies or can reasonably be used to identify the individual.
- PHI includes almost any health information that identifies the person, including demographic information.
- PHI can be electronic, written, or verbal information.



What is PHI?
18 Individual Identifiers

- Names
- All geographic subdivisions smaller than a state, including street address, zip code, etc.
- All elements of dates (except year) for dates related to the individual's birth date, admission date, discharge date, etc.
    - If the person is over age 89, all elements which indicate age must be removed
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Medical device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet protocol address numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

Minimum Necessary

- A CE must make reasonable effort to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

When May More than the Minimum Necessary be Used or Disclosed?

- When May More than the Minimum Necessary be Used or Disclosed?
  - When individual who is the subject of the PHI requests it;
  - Pursuant to individual's signed HIPAA-compliant authorization;
  - To a health care provider for treatment purposes;
  - To HHS for complaint investigation, compliance review or enforcement; and
  - As required by law (*e.g.*, reporting domestic abuse, court order, etc.)

What Uses and Disclosures are Permitted?

- Payment, Treatment and Health Care Operations
  - Payment includes:
    - Billing, claims management, obtaining payment;
    - Eligibility;
    - Coverage determinations; and
    - Appeals.
  - Health Care Operations include:
    - Quality assessments and improvement;
    - Auditing functions;
    - Legal services;
    - Business planning and development; and
    - Business management – mergers or consolidations.

What Uses and Disclosures are Permitted? (cont'd.)

- Public Policy and Safety Reasons if Authorized by Privacy Officer
  - Deceased persons;
  - Abuse, neglect, domestic violence, or endangerment situations;
  - Research – with notice;
  - Public health activities;
  - Health oversight activities;
  - Judicial and administrative proceedings;
  - Law enforcement purposes;
  - To avert a serious threat to health or safety;
  - Specialized government functions (national security activities); and
  - Organ, eye and tissue donation.
- A legal mandate enforceable in court that compels an entity to disclose PHI
  - The use and disclosure must comply with and be limited to the relevant requirements of such law.

Business Associate Agreements

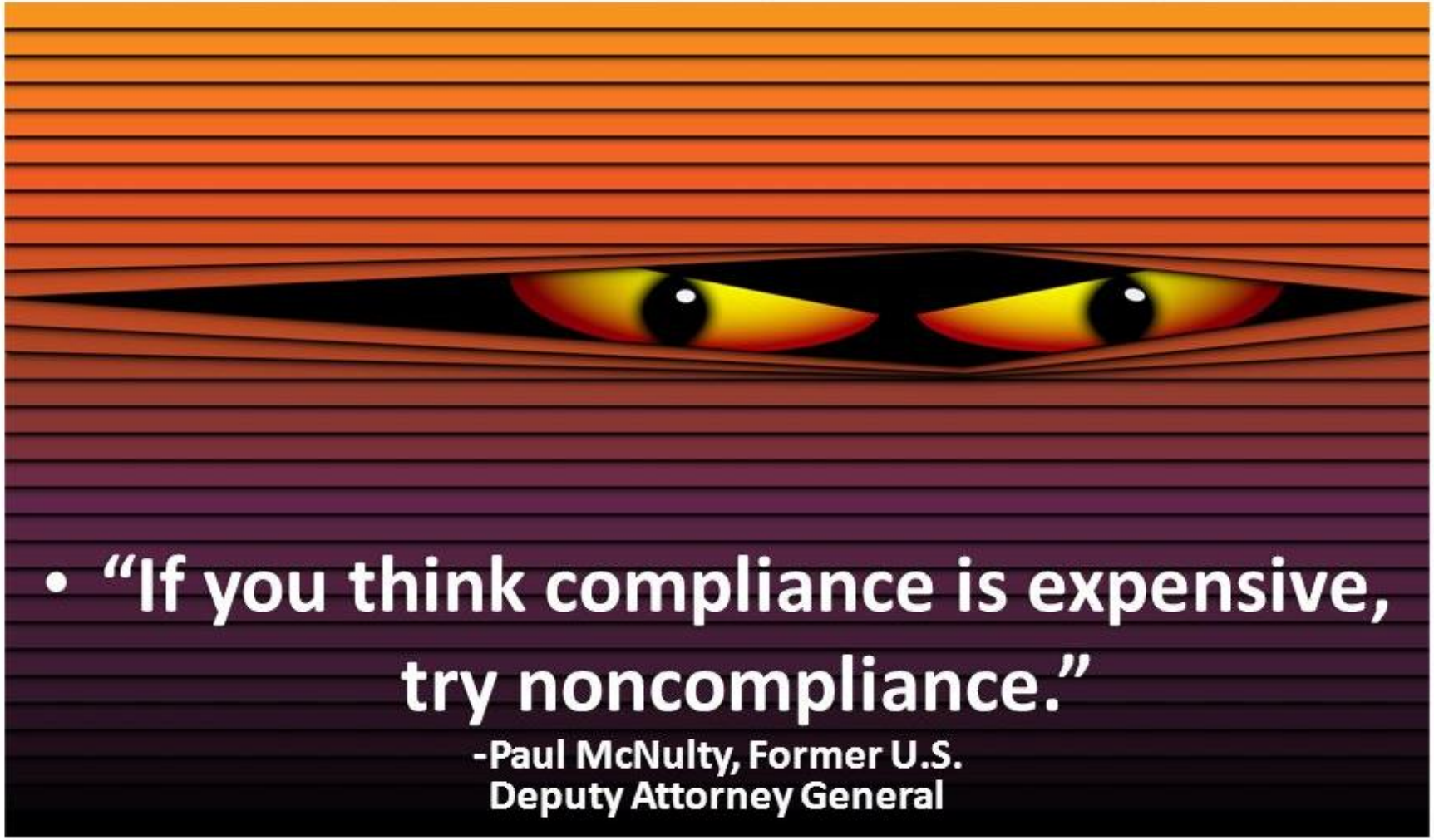
- When a vendor is a BA of a CE, both parties are required to enter into a written agreement with the vendor referred to as a BAA.
- The BAA provides that a vendor will safeguard PHI.
- A vendor is considered to be a BA based on its activity, not whether it has a BAA agreement in place.
- Vendors are often asked to sign BAAs in situations for which HIPAA isn't applicable.

"Business Associates are on the hook for HIPAA violations."

Business Associate Agreement

- The Center for Children's Digestive Health("CCDH") entered a settlement for $31K for failure to maintain a BAA with FileFax, Inc. in October 2016.
  - CCDH first began sharing PHI with FileFax in 2003, but the parties could not provide a signed BAA prior to October 12, 2015.
- Care New England Health System ("CNE") entered into a 400K settlement and CAP for acting as a BAA to its various entities under common ownership and control in September 2016
  - CNE provided centralized support for various entities such as finance, HR, IT, insurance, and compliance.
  - One such entity Women and Infants Hospital of Rhode Island (WIH) reported loss of unencrypted backup tapes containing ultrasounds for 14,000 patients.
  - OCR found that WIH had signed a business associate agreement with Care New England Health System, effective March 15, 2005, that was not updated until August 28, 2015, and therefore did not incorporate revisions required under the HIPAA Omnibus Final Rule.

PHI DATA BREACH IS LURKING



KUTAKROCK

What is a Breach ?

- Breach
  - A “Breach” is the:
    - Unauthorized acquisition, access, use, or disclosure of PHI;
      - Unsecured PHI triggers notification requirement;
    - Which compromises the security or privacy of such information.
  - There is a presumption of a Breach unless the Covered Entity or Business Associate can demonstrate that there is a low probability that the PHI has been compromised based on a four-factor risk assessment.

What is a Breach?

- Unauthorized acquisition, access, use, or disclosure:
  - Any use or disclosure not expressly required or permitted by the Privacy Rule;
  - Includes the sharing, release, or provision of PHI; and
  - Includes the intentional and unintentional acquisition, access, use, or disclosure of PHI.
- Unsecured PHI:
  - PHI is unsecured if the technology protection methods set out in HITECH (*e.g.*, encryption) are not used.
    - Must render the PHI unreadable, unusable, or indecipherable to unauthorized individuals

Breach Risk Assessment

- Four-Factor Risk Assessment. Determine:
  - The nature and extent of PHI involved, including identifiers and likelihood of re-identification;
  - Who impermissibly used the PHI or to whom the PHI was disclosed;
  - Whether and to what extent the PHI was actually acquired or viewed; and
  - The extent to which the risk has been mitigated.

Exceptions to a Breach

- Three Exceptions to General Breach Definition
  - The unintentional acquisition, access, or use of PHI by an employee if the acquisition was made in good faith, was within the scope of employment, and does not result in further use or disclosure.
    - *Example A*: An employee enters a coworker's office to drop off a document. The employee sees a document containing PHI on the coworker's desk. The employee notifies the coworker and does not use or disclose the information that she saw. This is not a breach.
    - *Example B*: A receptionist not authorized to access PHI decides to look through patient files to learn of a friend's treatment; the exception would not apply in this case because the access was not unintentional, done in good faith, or within the scope of authority. Notification would be required.

Exceptions to a Breach.

- Three Exceptions to General Breach Definition (cont'd.)
  - Inadvertent disclosures of PHI from an authorized person to another authorized person at the same Covered Entity or Business Associate if the information received is not further used or disclosed in an impermissible way.
    - *E.g.*, One authorized employee receives a misdirected email containing PHI from another authorized employee. The receiving employee immediately deletes the email, notifies the sending employee, and does not use or disclose the information in the email. This is not a breach.

Exceptions to a Breach.

- Three Exceptions to General Breach Definition (cont'd.)
  - The Covered Entity or Business Associate has a good faith belief that the unauthorized person would not reasonably have been able to retain the information.
    - *E.g.*, An authorized employee inadvertently sends a letter containing PHI to the wrong address. The letter is returned unopened, as undeliverable. This is not a breach because the authorized employee could conclude in good faith that the information was not retained by an unauthorized person.

Duty to Mitigate.

- Covered Entities and Business Associates have a duty to mitigate the harm that results from the improper use or disclosure of PHI. This duty may require:
  - Terminating service provider contracts; and
  - Taking appropriate personnel action.

Encryption Safe Harbor

- *"We love encryption, and those who use encryption love it, too. In the event of a breach, using encryption assures that the information is unreadable, unusable, or undecipherable, which basically, would qualify that entity for safe harbors under our breach notification rule."*

  - Leon Rodriquez, Former Director, Office of Civil Rights

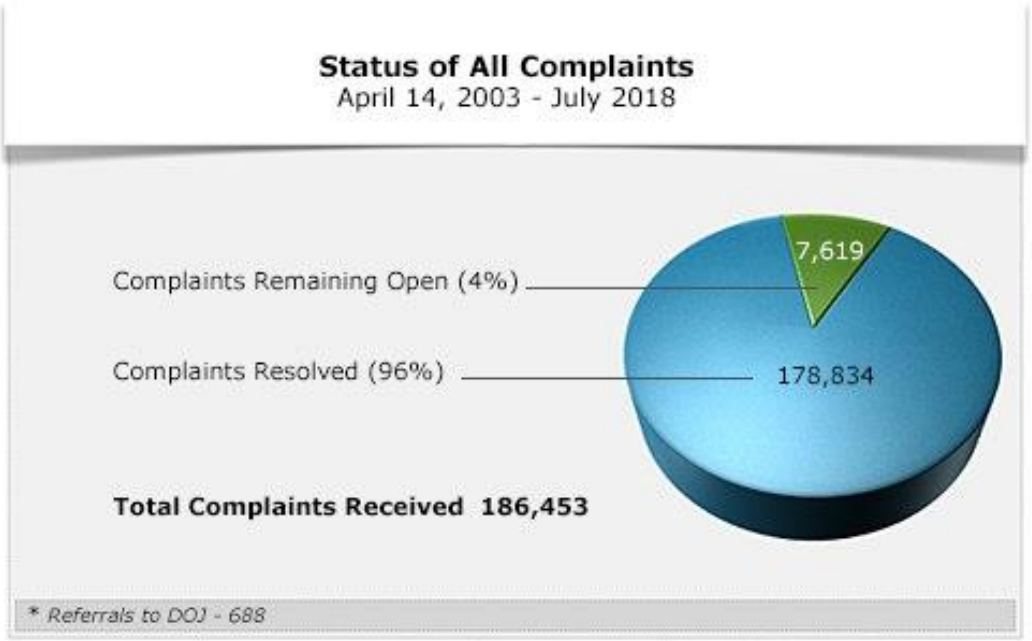
- If PHI is encrypted or otherwise rendered unreadable, unusable or indecipherable, pursuant to federal guidance, then no breach notification is required following an impermissible use or disclosure of the information.
  - **Encryption is a Safe Harbor to the HIPAA Breach Notification Rule**

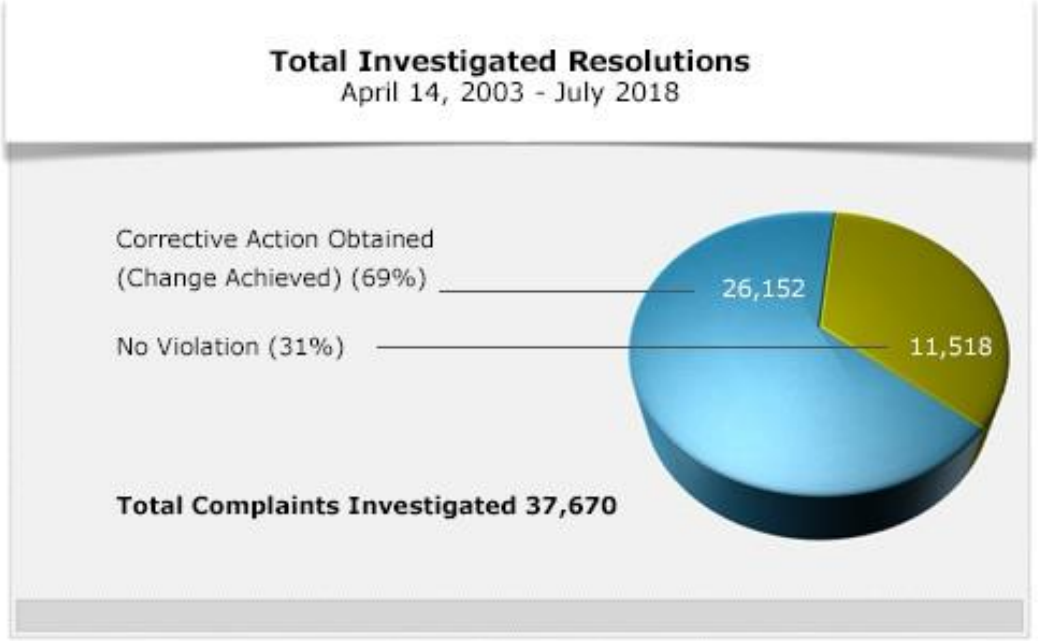
Examples of Potential Breaches

- Lost or Stolen USB stick containing PHI.
- Email string which has patient information or records sent or forwarded to the wrong recipient.
- Paper records left in a public place.
- A stolen laptop containing unencrypted PHI.
- An employee blogs about their workday which included specific patient diagnosis that can link to a patient.
- Someone has hacked into your EHR and obtained SSN for multiple patients.
- If you believe a Breach has occurred, you must notify the Privacy Officer IMMEDIATELY.

Theft & Loss are still the leading causes of health care data breaches

Numbers at a Glance





KUTAKROCK

Breach Notification Obligations

- Covered Entities are responsible to ensure notification in the event of a breach
  - Notification required without unreasonable delay, but in no case later than 60 days after breach discovery or when the breach should have been known.
    - Written notice to the affected individuals
    - If more than 500 individuals affected, notice to HHS
  - If more than 500 individuals affected in one state or jurisdiction, additional notice to the local media outlets.
  - Must also report annually to HHS for breaches affecting fewer than 500 individuals(report must be submitted no later than 60 days after the start of the calendar year following the year in which the breach occurred.)
  - BA must report a breach to the CE without unreasonable delay, and not later than 60 days after discovery, or in accordance with the terms of the applicable BAA if more stringent.

Recommendations in the Event of a Suspected Breach of Unsecured PHI

- Notify the Privacy or Security Officer and if applicable, IT staff, immediately in the event of a suspected breach, any authorized use or disclosure of PHI or a security incident.
- Individual staff should not independently determine whether a breach has occurred.
- Individual staff should not discuss incident details with anyone who does not have a need to know.
- Individual staff should not report a suspected breach directly to patients or the media under any circumstances.

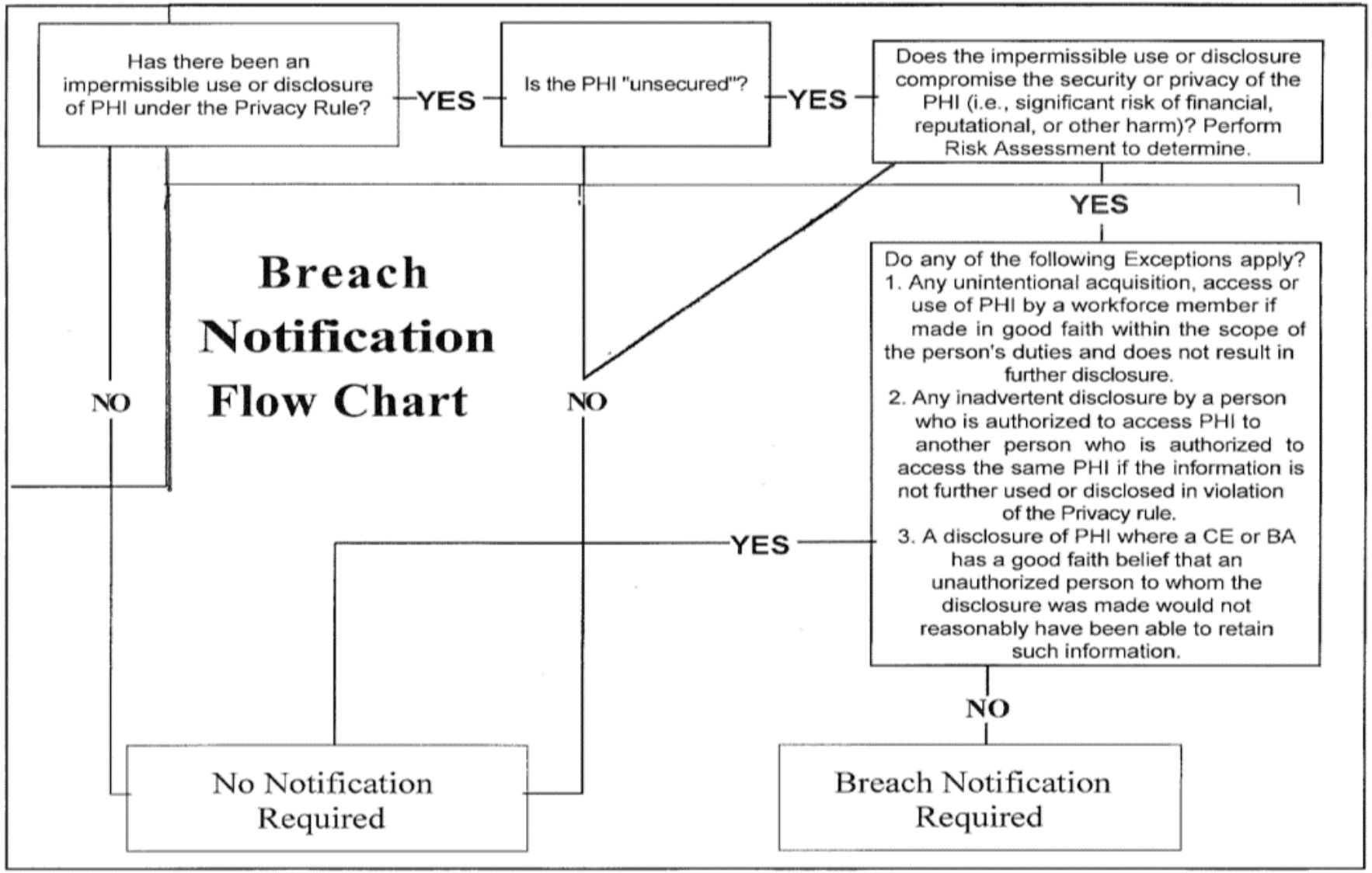
First HIPAA enforcement action for lack of timely breach notification settles for 475K

- The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced the first HIPAA settlement based on the untimely reporting of a breach of unsecured protected health information. Presence Health has agreed to settle potential violations of the HIPAA Breach Notification Rule by paying $475,000 and agreeing to implement a corrective action plan.
- On January 31, 2014, OCR received a breach notification report from Presence Health indicating that on October 22, 2013, Presence discovered that paper-based operating room schedules, which contained the PHI of 836 individuals, were missing from the Presence Surgery Center at the Presence St. Joseph Medical Center in Joliet, Illinois.
- The information consisted of the affected individuals' names, dates of birth, medical record numbers, dates of procedures, types of procedures, surgeon names, and types of anesthesia. OCR's investigation revealed that Presence Health failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the 836 individuals affected by the breach, prominent media outlets (as required for breaches affecting 500 or more individuals), and OCR.

What if a Breach Occurs?

Data Breach Requirements

- Investigation
  - Who
  - What
  - When
  - Where
  - Why
  - 4 Breach Risk Assessment Questions
- Notification
  - Individuals
  - Secretary of Health and Human Services
  - Media (> 500)
  - Business Associates
  - 60 Days from the Date of Discovery
  - No Unreasonable Delay
- Documentation
- Breach = YES
  - Documentation that shows all notification were made, Date of Notification, Content of Notification
- Breach = NO
  - Documentation from the Risk Assessment, low probability that the information was compromised
  - Application of any of the exceptions and why


Has there been an impermissible use or disclosure of PHI under the Privacy Rule?
YES
Is the PHI "unsecured"?
YES
Does the impermissible use or disclosure compromise the security or privacy of the PHI (i.e., significant risk of financial, reputational, or other harm)? Perform Risk Assessment to determine.
YES
Do any of the following Exceptions apply?
1. Any unintentional acquisition, access or use of PHI by a workforce member if made in good faith within the scope of the person's duties and does not result in further disclosure.
2. Any inadvertent disclosure by a person who is authorized to access PHI to another person who is authorized to access the same PHI if the information is not further used or disclosed in violation of the Privacy rule.
3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
NO
Breach Notification Required
Breach Notification Flow Chart
NO
NO
YES
No Notification Required

County Government Settles Potential HIPAA Violations-1st Settlement with Local Government

- Skagit County, Washington, agreed to settle potential violations HIPAA Privacy, Security, and Breach Notification Rules. Skagit County agreed to a $215,000 monetary settlement and to work closely with the Department of Health and Human Services (HHS) to correct deficiencies in its HIPAA compliance program.
- **Skagit County Had Insufficient Risk Management Policies**. The county allegedly failed to implement sufficient policies and procedures to prevent, detect, contain, and correct security violations;
- **Skagit County Had Insufficient Security Policies**. The county allegedly failed to implement and maintain documented policies and procedures reasonably designed to ensure compliance with the Security Rule; and
- **Skagit County Had an Inadequate Security Training and Awareness Program**. The county allegedly failed to provide appropriate security awareness and training to its workforce members, including its Information Security staff members.
- OCR also charged Skagit County with **violations** of the **Breach Notification** Rule based on finding that the county failed to notify all of the individuals whose ePHI had been compromised as a result of the breach.

Alaska DHSS settles HIPAA security case for $1,700,000

- Alaska Department of Health and Human Services (DHHS) has agreed to pay the U.S. Department of Health and Human Services' (HHS) $1.7 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule.
- Alaska also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of its patients' protected health information. OCR's investigation followed a breach report submitted by Alaska DHHS as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act.
- The report indicated that a portable electronic storage device (USB hard drive) possibly containing ePHI was stolen from the vehicle of a DHHS employee. Over the course of the investigation, OCR found that DHHS did not have adequate policies and procedures in place to safeguard ePHI.
- Further, DHHS had **not completed a risk analysis, implemented sufficient risk management measures, completed security training for its workforce members, implemented device and media controls, or addressed device and media encryption as required by the HIPAA Security Rule.**

HIPAA Resources

- Office of Civil Rights ("OCR") Website
  - https://www.hhs.gov/hipaa/index.html
- OCR FAQ
  - https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/index.html
- Missouri Department of Health and Senior Services Website
  - https://health.mo.gov/information/hipaa/

THANK YOU!

Marceda M. Starks, Of Counsel

Kutak Rock LLP

Telephone: 816-502-4621

marceda.starks@kutakrock.com

KUTAKROCK